Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=d38f9d09-4aa0-42ac-990c-252ee147f99a

MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Court Limits Right of Employers to Obtain Stored Text Messages from Vendors' Servers

June 2008
by Charles H. Kennedy

Related Practices:

- Employment and Labor
- Privacy and Data Security

In a decision entered on June 18, 2008, the United States Court of Appeals for the Ninth Circuit made important findings concerning the right of employers to obtain and read employees' text messages sent over employer-provided services. This Legal Update discusses the decision in detail and recommends that employers review their workplace surveillance practices to ensure their continuing compliance with state and federal law.

The Ninth Circuit's Decision

The decision in *Quon et al. v. Arch Wireless et al.* has its origins in an internal affairs investigation into text messages sent by members of the City of Ontario, California, Police Department.[1] Sergeant Jeff Quon had sent a number of messages to other persons, including Sergeant Steve Trujillo, Dispatcher April Florio, and Quon's wife, Jerilyn Quon, using an alphanumeric pager issued by the Department. The volume of messages sent from Quon's pager exceeded the service provider's limit of 25,000 characters per pager per month, causing the city to incur overage charges. The City of Ontario billed those charges to Quon and other individual employees who had exceeded the character limit.

In response to a complaint from the police lieutenant in charge of collecting overages, the Ontario police chief ordered an audit of Department members' pager usage to determine if the overages were incurred for official business. The contents of employees' text messages were stored on the server of the City's vendor, Arch Wireless. Pursuant to an email request from the City, Arch Wireless turned over transcripts of the text messages sent by certain employees, including Sergeant Quon, to the City. The internal affairs review of the transcripts disclosed that many of the messages were non-work-related, including messages that were "personal in nature and were often sexually explicit."[2]

Sergeant Quon, his wife, and two Department members with whom Quon exchanged messages brought a complaint against the City, Arch Wireless, the Chief of Police, the Department, and Sergeant Debbie Glenn, a member of Internal Affairs who had been involved in the investigation. Among other claims, the complaint alleged that the City and the Department had violated the plaintiffs' rights under the United States and California Constitutions when they obtained and read the stored text messages, and that Arch Wireless had violated the Stored Communications Act when it voluntarily surrendered the contents of the plaintiffs' text messages to the City.

The trial court (the United States District Court for the Central District of California) held that Arch Wireless did not violate the Stored Communications Act and that the governmental defendants did not violate the Fourth Amendment to the United States Constitution, which prohibits unreasonable searches and seizures.[3] The plaintiffs appealed those decisions to the Ninth Circuit.

The Ninth Circuit's Reading of the Stored Communications Act

The Stored Communications Act ("SCA") defines the circumstances under which persons may gain access to emails and other electronic communications that are stored on a service provider's facilities.[4] The SCA also governs a service provider's disclosure of those communications to

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=d38f9d09-4aa0-42ac-990c-252ee147f99a

others.[5]

In motions filed with the trial court, the plaintiffs had argued that as an electronic communication service provider to the public, Arch Wireless was prohibited by the SCA from "knowingly divulg[ing] to any person the contents of a communication while in electronic storage by that service."[6] The trial court disagreed, finding that Arch Wireless was a not an electronic communication service provider but a "remote computing service," which is permitted by the SCA to disclose the contents of stored communications on its server to its subscriber (in this case, the City of Ontario).[7]

The Ninth Circuit reversed the lower court on this point, finding that Arch Wireless's text-messaging pager service was not a remote computing service, which is defined in the SCA as "the provision to the public of computer storage or processing services,"[8] but an electronic communication service, which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[9] The Ninth Circuit based its conclusion on the statutory definitions, the SCA's legislative history, and the court's own 2004 decision in *Theofel v. Farey-Jones,* which characterized an email service provider's storage of messages after delivery as archival storage for backup protection by an electronic communication service provider.[10]

As a provider of electronic communication services, Arch Wireless was not permitted to release the contents of messages stored on its service to a mere "subscriber," such as the City of Ontario, but could divulge those messages only to "an addressee or intended recipient" of those messages.[11] Accordingly, the Ninth Circuit found as a matter of law that Arch Wireless's unauthorized disclosure of the contents of plaintiffs' text messages to the City was unlawful under the SCA.

The Constitutional Claims

The plaintiffs had also argued in the district court that the City, the Police Department and the Chief of Police had violated their rights under the Fourth Amendment to the U.S. Constitution, and that all of the defendants, including Sergeant Glenn, had violated their right to privacy under the California Constitution.

These claims, which were based upon the defendants' constitutional obligations as governmental bodies and agents, would not be available against private employers and will be discussed only briefly here.

The Fourth Amendment claim (and the California constitutional claim as well, to the extent that it was based upon a theory of unreasonable search and seizure) could succeed only if the plaintiffs had a reasonable expectation of privacy in the contents of their text messages and if the search or seizure was unreasonable.

On the first question, the district court had found that the plaintiffs *did* have a reasonable expectation of privacy in the contents of the text messages, notwithstanding a formal Department policy that disclaimed any such expectation, because of a superior officer's stated informal policy (apparently relied upon by Sergeant Quon) of not auditing pager usage so long as overages were paid. The Ninth Circuit agreed with this finding.[12]

However, the Ninth Circuit rejected the lower court's finding, pursuant to a jury verdict, that the seizure of plaintiffs' messages was reasonable. Although the Ninth Circuit accepted the jury's conclusion that the search was intended to "determine the efficacy of the 25,000 character limit," the court also found that the Department could have achieved that purpose by less intrusive means, rendering the seizure and reading of the text messages unreasonable. Accordingly, the Ninth Circuit found that the search violated the plaintiffs' Fourth Amendment rights and the plaintiffs' privacy rights under the California Constitution.[13]

Implications of the Ninth Circuit's Decision

The *Quon* case contains lessons for employers and communications service providers alike.

For employers, *Quon* is a reminder of the importance of obtaining comprehensive, effective consent from their employees to monitor their communications over employer-provided facilities, and of avoiding statements and actions that might be construed as a weakening or outright waiver of those surveillance rights.

Notably, the record in *Quon* showed that Department employees were, in fact, subject to a

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=d38f9d09-4aa0-42ac-990c-252ee147f99a

"Computer Usage, Internet and E-mail Policy" stating that "[u]sers should have no expectation of privacy or confidentiality when using [Department-provided] resources."[14] Sergeant Quon had signed this written policy, and the Ninth Circuit conceded that this fact ordinarily would have defeated Quon's expectation of privacy in the contents of his text messages. However, *a lieutenant's informal policy of not auditing employees' messages, so long as those employees agreed to pay for overages, weakened the effect of the written policy sufficiently to create a reasonable expectation of privacy in Quon's messages.* The decision underscores the importance of ensuring that all managers in an organization stay "on message" where surveillance of employee communications is concerned.[15]

The decision is also a reminder that an employee's consent to monitoring of communications by the employer may not, by itself, enable the employer to obtain an employee's stored communications from a third-party vendor. In order to foreclose this problem, it may not be necessary for all employers to provide their own communications services and store all employee communications on their own servers; but employers that use third-party vendors should consider, in light of *Quon,* whether they should obtain each employee's consent to the vendor's disclosure, to the employer, of the contents of all messages as to which the employee is the originator, addressee, or an intended recipient.

Finally, *Quon* should remind email providers and other electronic communication service providers of their special privacy obligations under state and federal electronic surveillance laws, including the Stored Communications Act. When those service providers furnish communication services for employees on behalf of an employer, it is natural to regard the employer as the customer and to treat that customer's demands as paramount. However, as *Quon* shows, statutory obligations to protect the privacy of employees may in some cases supersede the employer's rights, and failure to understand and comply with those obligations can lead to legal liability for the service provider.

Conclusion

The *Quon* decision underscores the complexity of the laws governing electronic surveillance of, and access to, employees' electronic communications. Morrison & Foerster's privacy team will be happy to provide further advice and assistance on these issues.

Footnotes

[1] *Jerilyn Quon; April Florio; Jeff Quon; Steve Trujillo, Plaintiffs-Appellants v. Arch Wireless Operating Company, Incorporated, a Delaware Corporation; City of Ontario, a Municipal Corporation; Lloyd Scharf, individually and as Chief of Ontario Police Department; Ontario Police Department; Debbie Glenn, individually and as a Sergeant of Ontario Police Department, Defendants-Appellees,* No. 07-55282, D.C. No. CV-03-00199-SGL (9th Cir. June 18, 2008)("Quon Slip Op.").
[2] Quon Slip. Op. at 7007.
[3] A trial was held on the Fourth Amendment claim, limited to the question of the police chief's intent in ordering the search. The trial court's other findings were made in the course of rulings on motions.
[4] 18 U.S.C. § 2701 *et seq.*
[5] *Id.* § 2702.
[6] *Id.* § 2702(1).
[7] *See id.* § 2702(b).
[8] *Id.* § 2711(2).
[9] *Id.* § 2510(15).
[10] *Theofel v. Farey-Jones,* 359 F.3d 1066, 1070 (9th Cir. 2004).
[11] *Id.* § 2702(b)(1). An electronic communication service provider also may disclose the contents of users' communications in certain other circumstances, including "with the lawful consent of the originator or an addressee or intended recipient of such communication," but the plaintiffs had not given such consent.
[12] The Ninth Circuit separately analyzed the privacy expectations of Trujillo, Florio, and Jerilyn Quon. The court noted that the three could not have complained if Sergeant Quon had voluntarily disclosed the contents of messages to which they were parties, or had given the Department permission to review those messages. However, those plaintiffs "had a reasonable expectation that the Department would not review their messages absent consent from either a sender or recipient of

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=d38f9d09-4aa0-42ac-990c-252ee147f99a

the text messages." Slip Op. at 7021.

[13] The court rejected an argument that Quon's expectation of privacy was unreasonable because of the possibility of public disclosure of the contents of his messages under the California Public Records Act. The Ninth Circuit also considered claims of qualified and statutory immunity from constitutional claims that are not discussed here.

[14] Slip Op. at 7022.

[15] It should be noted that the "reasonable expectation of privacy" analysis in *Quon* is based on a constitutional Fourth Amendment issue that is not ordinarily present in the private employment context. However, a court's analysis of the expectations created by a private employer's policy statements will often be quite similar to the "reasonable expectation" analysis called for by the Fourth Amendment.

© 1996-2008 Morrison & Foerster LLP. All rights reserved.